CYBERCUBE: EXPERIMENTS CAPABILITIES OVERVIEW

Prepared by	ESO CyberCUBE Team
	ESA

Document Type	TN - Technical Note
Reference	ESA-ESO-TN-2026-0073ESA-ESO-TN-2026-0073
Issue/Revision	1 . 0
Date of Issue	21/05/2026
Status	N/A

APPROVAL

Title	CyberCUBE: Experiments Capabilities Overview		
Issue Number	1	Revision Number	0
Author	ESO CyberCUBE Team	Date	21/05/2026
Approved By		Date of Approval	

CHANGE LOG

Reason for change	Issue Nr	Revision Number	Date

CHANGE RECORD

Issue Number	1	Revision Number	0
Reason for change	Date	Pages	Paragraph(s)

DISTRIBUTION

Name/Organisational Unit

Table of Contents

1. INTRODUCTION

The CyberCUBE mission will provide a real-world demonstration of sophisticated data analysis tools designed to **detect and counter potential cyber threats**. In response to the growing need for stronger space cybersecurity, the project will deliver a cutting-edge in-orbit operational laboratory equipped with innovative onboard cyber capabilities.

The project encompasses a 3U cubesat, equipped with advanced reprogrammable processing capabilities and a core payload for cybersecurity monitoring. The platform will remain operational in orbit for at least one year, collecting essential data on space asset vulnerabilities and cyber resilience.

The CyberCUBE architecture provides a comprehensive, flexible, and secure environment capable of **supporting advanced space experiments** and resilient communication. The integration of reconfigurable hardware, robust security protocols, fault tolerance, and specialized communication channels positions CyberCUBE as a state-of-the-art platform for secure, dynamic satellite missions aligned with ESA's high standards for space security and operational robustness.

CyberCUBE is in polar sun synchronous orbit.

Figure 1 CyberCUBE mission logo and patch

1.1. Scope

This document describes CyberCUBE's features highlighting the functions and possibilities that the mission offers to experimenters.
It aims to offer a view of the technical capabilities and to support a call for ideas, in order to perform experiments during the mission. As such, it does not provide all system architecture details and more detailed information that will be shared only with the selected experimenters

1.2. Acronyms and abbreviations

API	Application Programming Interface
CSOC	Cyber Security Operational Center
FPGA	Field Programmable Gate Array
GSE	Ground Support Equipment
LEO	Low Earth Orbit
HSM	Hardware Security Module
HW	Hardware
MCS	Mission Control System
OBC	On-board Computer
OBSW	On-board Software
PGS	Payload Ground Segment
PUS	Packet Utilization Standard
RF	Radio Frequency
SCCoE	Space Cyber-Security Center of Excellence
SLSP	Space Data Link Security
SVF	Software Validation Facility
SW	Software
TEE	Trusted Execution Environments
TMTC	Telemetry and Telecommand
TTC	Telemetry, Tracking and Command

2. TECHNICAL FEATURES

2.1. On Ground architecture overview

The following figure shows the high-level architecture of the CyberCUBE ground segment. As the mission's central connectivity hub, the SCCoE integrates a suite of utilities supporting mission operations and serves as the core node for the mission. It functions as a comprehensive monitoring and management platform for experiments, overseeing their entire lifecycle, from testing phases and status updates to results and version histories.
As shown in the image below, there are two separate communication links: one for the payload and one for TTC. The payload link is managed by the ESOC Ground Segment, while the TTC link is managed by the ESEC Ground Segment.

The SCCoE environment is also providing access to the FlatSat (fully representative the CyberCUBE's payload) that can be used to develop, test and validate the experiments before to run them on the CubeSat.

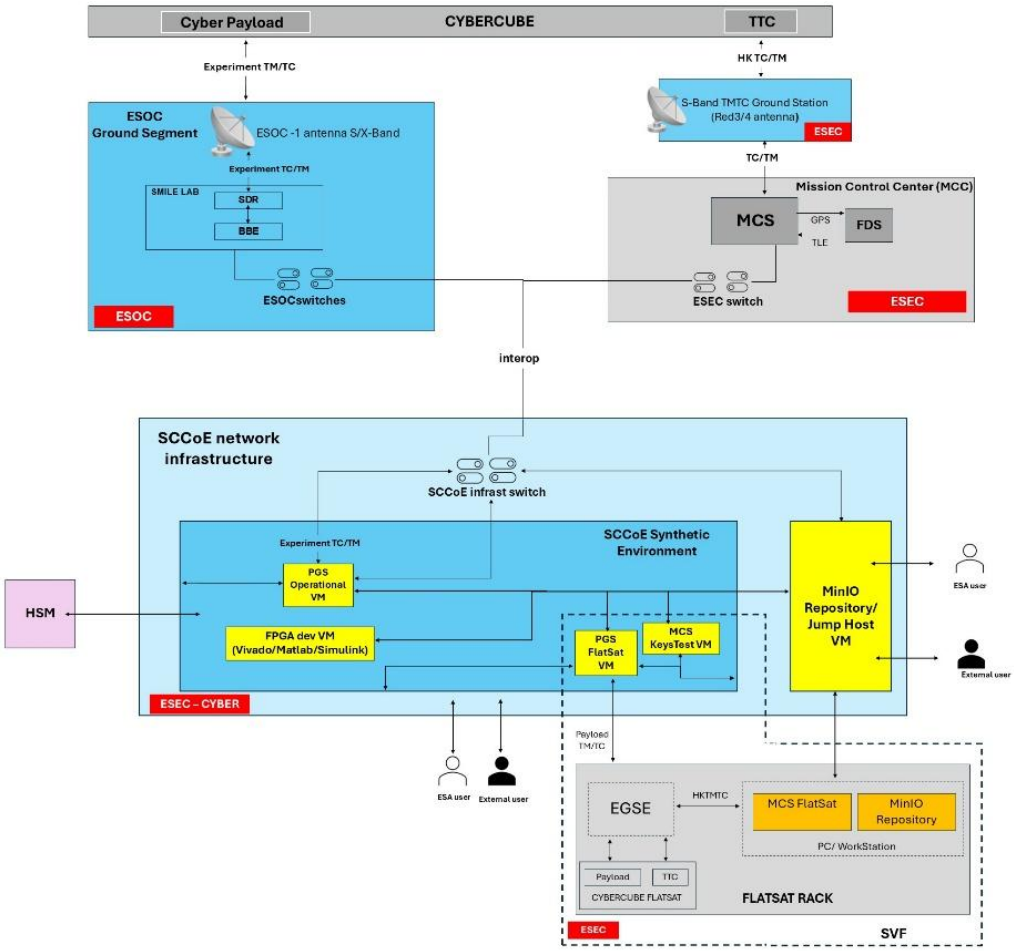

Figure 2 CyberCUBE Ground Segment

2.1.1. ESA Space Cyber-Security Center of Excellence (SCCoE)

The **ESA Space Cyber-Security Center of Excellence** (**SCCoE**) shall act as the central place for dealing with experiments, and as the main interface point for external access to the overall system and its capabilities.

SCCoE serves as management system for the experiments. Its responsibilities encompass tracking the lifecycle of each experiment, including its testing phases, status updates, results, and version histories, regardless of whether the experiments are conducted directly within SCCoE or in external partner labs.

For this purpose, SCCoE will provide remote connectivity to facilitate interaction with external experimenters. This capability will enable researchers and collaborators from outside the ESA ecosystem to access and interface with the SCCoE infrastructure, contributing their experiments and leveraging its centralized monitoring and management systems

2.1.1.1. The SCCoE Synthetic Environment

Within the SCCoE Synthetic Environment (SE) every tool is installed on a dedicated Virtual Machine (VM).
As shown in the previous figure, the SCCoE Synthetic Environment consists of four VMs (highlighted in yellow), each hosting specific tools and services:

- PGS Operational VM: The PGS is a specialized software designed to monitor, manage, and control the operations of the CyberCube Payload.
- PGS FlatSat VM: an identical copy of the PGS Operational VM, dedicated to monitor, manage, and control the operations of the FlatSat Payload
- FPGA dev VM: The FPGA development environment is provided as a virtual machine that contains AMD Vivado™ Design Suite and Vitis Model Composer for FPGA programming, hardware design, and model-based development of FPGA-based experiments. It also provides MATLAB, Simulink, DSP System Toolbox, and Signal Processing Toolbox to support algorithm development, signal processing simulation, and validation activities.

The MinIO Repository/Jump Host VM serves as the central storage service for transferring data and files into and out of the SCCoE. It provides a unified platform that supports drag-and-drop exchange through its graphical interface, enabling efficient management and sharing of data and files among the VMs within the SCCoE SE and external users.

2.1.2. System Validation Facility (SVF)

The SCCoE is responsible for coordinating the transfer and validation of experiments within the System Validation Facility (SVF), where they are executed on the FlatSat.

The SVF represents the most representative end-to-end environment of both ground and flight segments and includes:

- The Experiment MinIO Repository, used to store experiments and maintain the history of uploaded packages and results
- The SVF Mission Control System, used to interface with the FlatSat OBC
- The SVF Payload Ground Segment, used to interface with the FlatSat payload
- The FlatSat and its associated GSE, fully representative of the in-orbit CyberCUBE platform and used for integration, compatibility, and operational validation activities

The FlatSat reproduces the complete satellite subsystem configuration in a laboratory environment, enabling system-level testing and validation before deployment in orbit.
As a result, external experimenters can access the FlatSat through the SCCoE to develop, test, and validate their experiments before uploading them to the CyberCUBE payload.

2.2. Payload architecture overview

The CyberCUBE HW/SW Processing Infrastructure Architecture is designed as a robust, reconfigurable platform that supports hardware and software upgrades while maintaining security and operational integrity.
The reconfigurable HW/SW framework enables dynamic patching and **FPGA reprogramming** through Dynamic Partial Reconfiguration, allowing selective reconfiguration of FPGA areas. This functionality ensures certain FPGA regions remain immutable for secure operations, while user-reconfigurable areas are available for experiments or additional functionalities. This architecture enhances flexibility, enabling the CyberCUBE system to adapt to diverse mission requirements.
At the core of experiment management is the Experiments Manager, which provides a supervisory layer over experiments conducted on the CyberCUBE SoC. This interface allows seamless **control of experiment-related tasks** and interactions with onboard resources,

facilitating efficient data collection and analysis. Complementing this, the Payload Driver integrates with the Analog-to-Digital (AD) Software-Defined Radio, which is part of the Transceiver Receiver and Exciter Volume (TREVO). This component enhances data acquisition and processing capabilities, supporting various communication needs.

The Hypervisor Virtualization Layer, utilizing a Xen Hypervisor, offers Time and Space Partitioning across different operating systems, including Linux, petalinux, FreeRTOS, and RTEMS. This layer enables **secure resource allocation and isolation**, supporting advanced architectures like Trusted Execution Environments (TEE). The hypervisor's flexible architecture enables CyberCUBE to adapt its security profile dynamically to meet evolving mission requirements and threats.

Security is a foundational component of the CyberCUBE, with several verifiable security techniques embedded within the architecture. A Hardware Security Module (HSM) IP core provides secure cryptographic functions, including key derivation, secure storage, etc. This secure architecture ensures that sensitive cryptographic operations are isolated and protected. The use of XMSS (eXtended Merkle Signature Scheme) signatures provides compact and **secure digital signatures** suitable for the CyberCUBE's resource-constrained environment, ensuring that code signing and firmware updates maintain integrity throughout the satellite's lifecycle. FPGA HW security blocks in the Zynq Ultrascale+ enable secure booting and support cryptographic operations, utilizing built-in cores for AES, RSA, SHA, and Physically Unclonable Functions (PUF), among others, making it a **versatile platform** for secure space applications. The hardware protection mechanisms include Secure Boot to prevent unauthorized code execution and a Root of Trust (RoT) module to establish a secure anchor for all system processes, ensuring only verified firmware is loaded.

RF Interference Monitoring on the S-band payload link allows for proactive interference detection, critical for maintaining **secure and efficient satellite operations**.

Experiment data, including new software images or FPGA updates, can be uploaded directly to the Payload via the Payload S-band SDR link based on CCSDS SDLS TM/TC protocol. Dedicated channels within the CyberCUBE payload allow experiments to transmit data without overloading the main TTC link, preserving the OBC's command authority. This guarantees a physical segregation between platform and payload.

The payload is also hosting a X-band transmitter based on DVB-S2 protocol for high data rate download.

The functionality of downloading images taken with the Earth sensor through the X-Band transmitter is included.

In summary, the CyberCUBE payload architecture provides a comprehensive, flexible, and secure environment capable of supporting advanced space experiments and resilient communication. The integration of reconfigurable hardware, robust security protocols, fault tolerance, and specialized communication channels positions CyberCUBE as a state-of-the-art platform for secure, dynamic satellite missions aligned with ESA's high standards for space security and operational robustness.

2.3. Payload communication capabilities

For the CyberCUBE mission, the satellite will carry one payload assembled in a single stack, including the following elements:

- TREVO SDR
- S-band Front-End
- X-band transmitter
- S-band antenna
- X-band antenna

The payload is managed by the modular high-performance TREVO Software Defined Radio platform. This radio is configured in this mission with 1x SoC and 1xTRX module, placed on TREVO's motherboard, which provides electrical and mechanical support to the modules. The SoC module, consisting on a 5EG device Zynq UltraScale+ MPSoC, provides the application processors and programmable logic tools required for cyber experiments of this project. The

TRX module allows DAC/ADC conversion of incoming/outcoming signals from the SDR for RF communications, via the AD9361 transceiver.

The CyberCube payload has two different communication chains with ground segment:

1) S-band with uplink and downlink communications
2) X-band with downlink only communication

2.4. Payload Communications

2.4.1. S-band Interface

The TREVO S-band link is used to communicate directly between Ground and the CyberCUBE spacecraft. This communication link is used to upload commands and experiments directly to the Payload and downlink telemetry and experiment data (such as experiment status information), without involving the Platform OBSW and TTC.

The S-band communication is bidirectional, and its stack is reported in the table below.

OSI reference layer	Mnemonic	CCSDS layer	Protocol	Implementation
Presentation	CFDP	File Delivery Protocol	CCSDS 727.0.B-5 File Delivery Protocol	PS
Network	PUS	Space Packet Protocol	ECSS-E-ST-70-41C (1)	PS
Data link	TMTC with SDLS (and SDLS EP)	Data Link protocol sublayer	CCSDS 355.0-B-2 Space Data Link Security Protocol	PL
		Synchronization and channel coding sublayer	ECSS-E-AS-50-24C (2)	PL
Physical	RF	Physical Layer	ECSS-E-ST-50-05 (3)	PL

Note (1): Based on CCSDS 133.0-B-1

Note (2): Substitutes ECSS-E-ST-0-04C. Based on CCSDS 231.0-B-3

Note (3): Based on CCSDS 401.0-B-17

Note: CyberCUBE accomodates several PUS services, both Standard and Private.

2.4.2. X-Band Interface

Cybercube will use X-band to download large amount of data generated by the payload to the ground station.
The protocol stack used for X-band downink is presented in the table below:

OSI layer	CCSDS layer	CCSDS Protocol	Standard
Network and Upper Layers	Network and Upper Layers		
Data Link Layer	Data Link Protocol Sublayer	TM Space Data Link Protocol	CCSDS 132.0-B
	Synchronization & Channel Coding Sublayer	SMTF Stream Generation	CCSDS 131.0-B
Physical Layer	Physical Layer	DVB-S2 Transmission	ETSI EN 302 307 V1,4,1 (2014-11)

2.5. Payload Onboard capabilities

Main features:

- Processing System (**PS**)
    - Payload Manager: is the central piece of software running on the TREVO SoC. The Payload Manager refers to the whole software running the TREVO to manage the payload meanwhile the experiment manager is a specific functionality within the Payload Manager. It is executed in the main domain of the

Xen hypervisor, running on the A53 processor. The payload manager is in charge of ensuring communication to and from the Platform, coordinating communication between the experiments and ground as well as providing housekeeping information regarding the Payload

- Mode Manager: acts as orchestrator for the whole payload considering the system and sub-system mode received from the OBC.
- Experiment manager: responsible for handling the existing experiments on the satellite. It ensures the storage of the experiments and their data, control over the experiments and access for the experiments to the required functionalities on board.
- Monitoring: provides services to monitor the CAN bus, the CPU usage and the memory usage.
- RF Interference: monitors and stores raw IQ samples from AD9361.
- CSP: Cubesat space protocol implementation
- CFDP: CCSDS File Delivery Protocol implementation
- Storage: provides storage services to the experiments.
- PUS: implements a subset of the standard PUS Services as well as a set of private PUS Services.
- HSM: Implements the Extended procedures from the Space Data Link Security Protocol including Device Identification, Key Negotiation and Key Derivation.
- CAN: Driver to manage the CAN interface
- S-Band: Driver managing the interface to the S-Band management in the FPGA.
- X-Band: Driver managing the LVDS interface to the X-Band transmitter.

- Programmable Logic (**PL**)
  - HSM: Includes a set of crypto cores available for the payload: ECDSA P-256, SHA3 512, HMAC, XMSS, ML-KEM, TRNG, SHAKE, RSA 1024 and AES-GCM.
  - SDLS: Implements the Space Data Link Security Protocol.
  - TM/TC: Manage telemetry and telecommands at frame level. It relies on the SDLS IPcore for the encryption and decryption.
  - S-Band Sync and Coding: synchronization and coding layer in the S-Band link.

- LVDS: Provides interface to the X-Band transmitter.
- libIIO: Provides raw access to IQ samples from the AD9361.

- Experiment execution: three types of experiment can be run on board:
  - Dom0 executables experiments
  - DomU Linux experiments
  - R5 Baremetal experiments

  Each type of experiment can have access to four different API sockets:
  - Storage API provides an interface through which data created during runtime can be downloaded when the Payload enters the X-Band transmission mode.
  - S-Band API allows experiment data to be forwarded to Ground. Experiments are identified with an APID. The format of the packets is CCSDS.
  - Crypto API provides access to cybersecurity services (see below)
  - Platform monitoring API forwards necessary details for forwarding data pool parameters to and from experiments. All the information exchanged from the platform and the payload is available for the experiments. As explained before, each FM/SW patch is signed using XMSS

- Reconfigurable HW/SW Framework: this capability enables software patching and FPGA re-programming using Dynamic Partial Reconfiguration. The FPGA dynamic partition can be used to host an FPGA-based experiment

- FPGA HW security blocks (HSM) featured with secure booting capabilities and hardware cores implementing cryptographic algorithms such as AES, RSA, SHA, Physically Unclonable Function (PUF), FPGA Secure Storage and eFUSE. It would provide a versatile platform for conducting experiments and implementing advanced security features in space applications.

- Cybersecurity services: include a list of available cryptographic functions and primitives:
  - Key Negotiation protocol, based on ML-KEM

- PKI functionalities: request a certificate and verify a certificate
- Key Management
- Key Derivation
- Crypto algorithms
  - AES GCM
  - RSA 1024
  - HASH functions (SHA3, SHAKE 128,256)
  - HMAC-SHA3-512
  - ECDSA P-256
  - ML-KEM_512
  - ML-KEM_768
  - ML_512 ENCAP
  - ML_768 ENCAP
  - XMSS
  - Pseudo and True RNG

- FPGA-based IP Core implementing the CCSDS SDLS (Space Data Link Security) protocol will be used.

- Monitoring functionalities:
  - Dedicated CAN bus/CPU/Memory monitoring service is implemented within the CyberPayload to potentially detect anomalous behaviour
  - RF interference: It utilizes the hardware capabilities of the AD9361 to acquire IQ files from digitized RF signals, enabling the capture and analysis

3. MISSION TIMELINE

CyberCUBE is set to be launched on the SpaceX Rideshare Transporter 17, targeting July 2026, and it will be released in a sun-synchronous orbit at an altitude of 590km.

After the launch, a couple of days of early operations are foreseen, and then the commissioning phase, as per Figure 3.
The mission is expected to be nominally operational about 1 month after launch: experiments shall not be performed before this time.

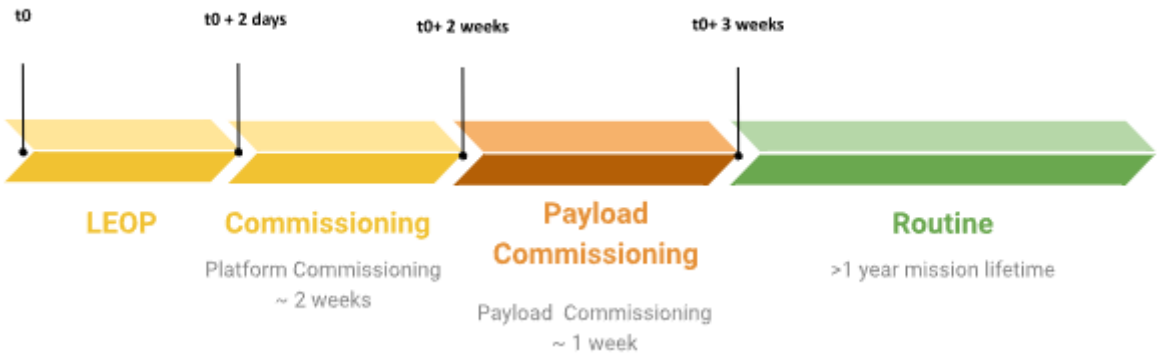

Figure 3 Concept of Operations timeline

The mission is expected to be operational for at least 1 year.